Construction of wiretap codes from ordinary channel codes

Masahito Hayashi
Graduate School of Information Sciences, Tohoku Univ., Japan
CQT, National Univ. of Singapore, Singapore
Email: hayashi@math.is.tohoku.ac.jp

Ryutaroh Matsumoto
Dept. of Communications and Integrated Systems,
Tokyo Institute of Technology, 152-8550 Japan
Email: ryutaroh@rmatsumoto.org

***Abstract*—From an arbitrary given channel code over a discrete or Gaussian memoryless channel, we construct a wiretap code with the strong security. Our construction can achieve the wiretap capacity under mild assumptions. The key tool is the new privacy amplification theorem bounding the eavesdropped information in terms of the Gallager function.**

I. Introduction

The information theoretical security [15] recently has attracted huge interest. The wiretap channel [7], [21] is one of its fundamental problems. On a wiretap channel, signals from the legitimate sender, called Alice, is delivered to both legitimate receiver, called Bob, and eavesdropper, called Eve. The goal of Alice is to deliver messages to Bob with low decoding probability while keeping Eve from knowing much about the messages. The capacity of wiretap channels has been determined for discrete memoryless channels [7], [21] and for Gaussian channels [14] with a weaker notion of security. The capacity of the above wiretap channels are also determined with a stronger notion of security [2], [6], [11]. The exponential decreasing rate of eavesdropped information is also evaluated in [11], [12]. Shannon theoretic study of the wiretap channels is fairly advanced.

On the other hand, there is still room for research in the actual construction of codes for the wiretap channels, which we call the wiretap codes. Thangaraj et al. [20] proposed an LDPC based construction for specific discrete memoryless channels, and Klinc et al. [13] proposed another LDPC based construction for Gaussian channels. Hamada [10] and Hayashi [12] proposed general linear code based construction for additive discrete memoryless channels. Muramatsu and Miyake proposed a construction based on the hashing property of LDPC matrices [18], whose decoding requires the high-complexity minimum entropy decoder.

In those constructions except [12], error correction and provision of secrecy are combined in the constructed coding scheme. This prevents us from using well-studied error-correcting codes for the error correction in the wiretap codes, and we need to adjust existing error-correcting codes or invent a new wiretap code. This inconvenience may not be necessary. In fact, in the quantum key distribution protocols, the error correction and the provision of secrecy can be separately studied and developed, see [16] and references therein.

Moreover, previous constructions for discrete memoryless channels do not cover all the discrete memoryless channels except [18]. It is desirable to have a construction of wiretap codes that can be used for any discrete memoryless channels.

In this paper, we show two constructions of wiretap codes from encoder and decoder in an ordinary channel code. We do not modify the channel encoder nor decoder. We attach the two-universal hash function to the encoder and the decoder in order to realize secrecy from Eve. We show that our construction can achieve the wiretap capacity in the *strong* security sense over discrete and Gaussian memoryless channels, while some of previous constructions do not have proofs of the strong security.

The key tools for our constructions are the new forms of the privacy amplification (PA) theorem [3]. The original PA theorem [3] does not achieve the optimal rate of PA, which is the conditional Shannon entropy of Alice's information conditioned on Eve's information. Renner [19] improved it so that Renner's version of the theorem can achieve the optimal rate. However, it does not enable us to construct the wiretap code using an existing channel code. The reason is that we cannot numerically compute the necessay rate of hashing for a given channel code in order for Eve's information on secret message to become sufficiently small. So we present two new forms of the PA theorem. One is already given in [12]. However, it requires the random selection of a chennel encoder from the given family of channel codes. We shall provide another form of the PA theorem in Theorem 7, which enables us to construct a wiretap code from single channel encoder. Our new PA theorem is a nontrivial adaptation of the channel resolvability lemma [11, Lemma 2].

This paper is organized as follows: In Sec. II we fix notations used in this paper. In Secs. III and IV two constructions of wiretap codes are given. In Sec. V we present a novel privacy amplification theorem bounding the eavesdropped information in terms of the Gallager function. Section VI concludes the paper.

II. Preliminary

In this section we shall fix notations used in this paper and review necessary prior results. Let $\mathcal{X}$ be the finite alphabet of channel inputs, $\mathcal{Y}$ the alphabet of channel outputs to the legitimate receiver, called Bob, and $\mathcal{Z}$ the alphabet of channel outputs to the eavesdropper, called Eve. The legitimate sender is called Alice. We fix the conditional probability or conditional probability density $Q_{Y|X}$ of the channel to Bob and $Q_{Z|X}$ of the channel to Eve. We assume channels are memoryless and further assume that

- both $\mathcal{Y}$ and $\mathcal{Z}$ are finite, which means that the channels are discrete memoryless,
- or $\mathcal{Y} = \mathcal{Z} = \mathbf{R}$ and the channels are additive Gaussian.

Let $\mathcal{M}_n$ be the set of messages transmitted to Bob secretly from Eve, $\eta_{\mathrm{Alice},n}$ a stochastic map from $\mathcal{M}_n$ to $\mathcal{X}^n$ of a wiretap encoder, and $\eta_{\mathrm{Bob},n}$ a deterministic map from $\mathcal{Y}^n$ to $\mathcal{M}_n$. We use the natural logarithm instead of $\log_2$ for convenience.

Definition 1: A rate $R > 0$ is said to be achievable if there exists a sequence $(\eta_{\mathrm{Alice},n}, \eta_{\mathrm{Bob},n})$ of encoders and decoders such that

$$\lim_{n\to\infty} \Pr[M_n \neq \eta_{\mathrm{Bob},n}(\eta_{\mathrm{Alice},n}(M_n))] = 0,$$
$$\lim_{n\to\infty} I(M_n; Z_n) = 0, \quad \liminf_{n\to\infty} \ln |\mathcal{M}_n| \geq R,$$

where M_n is the uniform random variable over $\mathcal{M}_n$ and Z_n is the random variable for Eve's channel output from channel input $\eta_{\mathrm{Alice},n}(M_n)$. The supremum of the achievable rates is the capacity of the wiretap channel $(Q_{Y|X}, Q_{Z|X})$.

Note that we employ the strong security criterion introduced by Csiszár [6] and Maurer and Wolf [17]. The necessity for the strong security is given in [2], [17].

Proposition 2: [2], [6], [11] The capacity of the wiretap channel $(Q_{Y|X}, Q_{Z|X})$ is

$$\max_{P_T, P_{X|T}} [I(T;Y) - I(T;Z)]. \tag{1}$$

In the next section, we shall show a construction of wiretap encoder and decoder from arbitrary given channel encoder and decoder. In the construction, we assume that we are given $Q_{X|T}$ achieving the maximum of Eq. (1). Note that when the wiretap channel is Gaussian, it is degraded and we can take $T = X$ without losing the optimality. In the construction, we shall also use a family of the two-universal hash functions [5], which is reviewed next.

Definition 3: Let $\mathcal{S}_1$ and $\mathcal{S}_2$ be finite sets and $\mathcal{F}$ a subset of the set of all mappings from $\mathcal{S}_1$ to $\mathcal{S}_2$. The family $\mathcal{F}$ is said to be a family of two-universal hash functions if

$$\Pr[F(x_1) = F(x_2)] \leq 1/|\mathcal{S}_2|,$$

for all distinct x_1 and x_2 in $\mathcal{S}_1$, where F is the uniform random variable on $\mathcal{F}$.

III. Randomized construction of a wiretap code

A. Encoder and decoder

In this section we shall construct wiretap encoder and decoder from arbitrary given ordinary channel encoder and decoder. The construction in this section can achieve the wiretap capacity (1) if the uniform distribution on $\mathcal{T}$ realizes the wiretap capacity (1). The assumptions are:

- We know $Q_{X|T}$ achieving the maximum of Eq. (1). Denote by $\mathcal{T}$ the alphabet of T.
- We are given a family channel encoders $\mu_{\mathrm{Alice},n,g}$ indexed by $g \in \mathcal{G}_n$ mapping a message in the message set $\mathcal{L}_n$ to a codeword in $\mathcal{T}^n$ and a channel decoder $\mu_{\mathrm{Bob},n,g}$ mapping a received signal in $\mathcal{Y}^n$ to a message in $\mathcal{L}_n$. The channel encoder $\mu_{\mathrm{Alice},n,g}$ is a one-to-one map, and $\mathcal{T}^n$ is equal to the disjoint union of $\mu_{\mathrm{Alice},n,g}(\mathcal{L}_n)$ for $g \in \mathcal{G}_n$.
- We are given a family $\mathcal{F}_n$ of two-universal hash functions from $\mathcal{L}_n$ to $\mathcal{M}_n$, where $\mathcal{M}_n$ is the message set of the wiretap code.

Remark 4: The assumption on the channel encoders is usually met with linear codes. We usually use the codebook of a linear code whose codewords have zero syndrome. If we allow codebooks to have nonzero syndrome, then the family of codebooks with multiple syndromes constitutes the family of encoders $\{\mu_{\mathrm{Alice},n,g} \mid g \in \mathcal{G}_n\}$.

From these assumptions, we can construct a wiretap encoder, which is an extension of Hayashi's construction [12]. Choose a hash function F_n uniformly randomly from $\mathcal{F}_n$ and $G \in \mathcal{G}_n$. For a given message M_n to the wiretap encoder of code length n, choose a message L_n uniformly randomly from $F_n^{-1}(M_n) \subset \mathcal{L}_n$, and compute the codeword $T_n = \mu_{\mathrm{Alice},n,G}(L_n)$ from the channel encoder. Finally, compute the actually transmitted signal X_n by passing T_n to the artificial memoryless channel $Q^n_{X|T}$. The decoder maps a given received signal Y_n in $\mathcal{Y}^n$ to the message $F_n(\mu_{\mathrm{Bob},n}(Y_n)) \in \mathcal{M}_n$.

The random selection of F_n and G_n is a fatal problem because it requires sharing of common randomness between Alice and Bob. However, we shall show that $I(M_n; Z_n|F_n, G_n)$ can be upper bounded by an arbitrary positive number $\epsilon_1 \times \epsilon_2$, which means that at least $100(1-\epsilon_1)$% choices of $f_n \in \mathcal{F}_n$ and $g_n \in \mathcal{G}_n$ keep $I(M_n; Z_n|F_n = f_n, G_n = g_n)$ below ϵ_2. Thus the legitimate sender and receiver can agree on the random choice of f_n before transmission of the secret messsage M_n.

B. Evaluation of the eavesdropped information

It should be clear that the (block) average decoding error probability of the constructed wiretap code is lower than or equal to that of the underlying code $(\mu_{\mathrm{Alice},n,g}, \mu_{\mathrm{Alice},n,g})$ for $g \in \mathcal{G}_n$ regardless of random choices of F_n and L_n from M_n. The remaining task is evaluation of the eavesdropped information $I(M_n, Z_n)$, where Z_n is Eve's received signal on the channel input X_n. To do so, we introduce Hayashi's version of the privacy amplification theorem [12]

Proposition 5: Let L be the *uniform* random variable with a finite alphabet $\mathcal{L}$ and Z any random variable. If Z is not discrete random variable then the conditional probability of Z given L is assumed to be Gaussian. Let $\mathcal{F}$ be a family of two-universal hash functions from $\mathcal{L}$ to $\mathcal{M}$, and F be the uniform random variable on $\mathcal{F}$. Then

$$H(F(L)|F, Z) \geq \ln|\mathcal{M}| - \frac{|\mathcal{M}|^s \times \exp(\psi(s, P_{LZ}))}{s|\mathcal{L}|^s}$$

for $0 < s \leq 1$, where

$$\psi(s, P_{LZ}) = \ln \sum_z \frac{\sum_\ell P_L(\ell)(P_{Z|L}(z|\ell))^{1+s}}{P_Z(z)^s}.$$

If Z is conditionally Gaussian $\sum_z$ should be replaced by the integration and P_Z, $P_{Z|L}$ denote probability densities.

Remark 6: The above proposition is a combination of [12, Eq. (2)] and the argument in proof of [12, Theorem 2]. It was assumed that Z was discrete in [12]. However, when the conditional probability of Z given L is Gaussian, there is no difficulty to extend the original result. It should be also noted that the uniformity assumption on L is indispensable, otherwise the claim is false.

By the above proposition, for fixed $G = g \in \mathcal{G}_n$ we have

$$\begin{aligned} I(M_n; Z_n^g, F_n) &= I(M_n; Z_n^g|F_n) \\ &= H(M_n|F_n) - H(M_n|Z_n^g, F_n) \\ &\leq \ln|\mathcal{M}_n| - H(M_n|Z_n^g, F_n) \\ &\leq \frac{|\mathcal{M}_n|^s \times \exp(\psi(s, P^g_{L_n Z_n}))}{|\mathcal{L}_n|^s s} \qquad (2) \end{aligned}$$

for $0 < s \leq 1$, where $P^g_{L_n Z_n}$ is the joint probability distribution and Z_n^g is Eve's received signal with a fixed $g \in \mathcal{G}_n$

A major problem with the last upper bound (2) on $I(M_n; Z_n|F_n)$ is that for a given channel code it is practically impossible to numerically compute $\psi(s, P^g_{L_n Z_n})$. To overcome this difficulty we shall upper bound $\exp(\psi(s, P^g_{L_n Z_n}))$ by $\exp(\psi(s, P_{TZ}))$, where P_{TZ} is a joint distribution on $\mathcal{T} \times \mathcal{Z}$.

Let $T_g = \mu_{\mathrm{Alice},n,g}(L_n)$ that is a random variable on $\mathcal{T}^n$. Note that T_g is the uniform random variable on $\mu_{\mathrm{Alice},n,g}(\mathcal{L}_n) \subset \mathcal{T}^n$. By the assumption on the given family of channel encoders $\mu_{\mathrm{Alice},n,g}$, $g \in \mathcal{G}_n$, the convex combination of $\sum_{g \in \mathcal{G}_n} P_{T_g}/|\mathcal{G}_n|$ is the uniform distribution $\mathrm{Uniform}(\mathcal{T}^n)$ on $\mathcal{T}^n$. By the concavity of $\exp(\psi(s, \cdot))$ on the channel input probability distribution[1] [12, Lemma 1], we have

$$\begin{aligned} \frac{1}{|\mathcal{G}_n|} \sum_{g \in \mathcal{G}_n} \exp(\psi(s, P^g_{L_n Z_n})) &\leq \exp(\psi(s, Q^n_{Z|T} \mathrm{Uniform}(\mathcal{T}^n)) \\ &= \exp(n\psi(s, Q_{Z|T} \mathrm{Uniform}(\mathcal{T})). \end{aligned}$$

Observe that computation of the last mathematical expression is easy for almost all channels.

What we have proved is

$$I(M_n; Z_n|F_n, G_n) \leq \frac{|\mathcal{M}_n|^s \times \exp(n\psi(s, Q_{Z|T} \mathrm{Uniform}(\mathcal{T})))}{|\mathcal{L}_n|^s s}. \qquad (3)$$

Observe that the minimization of the RHS of Eq. (3) over s is also computable by the bisection method [4, Algorithm 4.1] because it is convex with respect to s. The logarithm of the right hand side is

$$s\left(\ln|\mathcal{M}_n| - \ln|\mathcal{L}_n| + \frac{n\psi(s, Q_{Z|T}\mathrm{Uniform}(\mathcal{T}))}{s}\right) - \ln s. \qquad (4)$$

By l'Hôpital's theorem, we have

$$\lim_{s \to +0} \frac{\psi(s, Q_{Z|T}\mathrm{Uniform}(\mathcal{T}))}{s} = I(\mathrm{Uniform}(\mathcal{T}), Q_{Z|T}),$$

where the right hand side is the mutual information between the channel output and the uniform channel input to the imaginary channel $Q_{Z|T}$. Thus, by choosing s such that $\frac{\psi(s, Q_{Z|T}\mathrm{Uniform}(\mathcal{T}))}{s} < I(\mathrm{Uniform}(\mathcal{T}), Q_{Z|T}) + \delta$, we can see that if $\ln|\mathcal{M}_n| < \ln|\mathcal{L}_n - n(I(\mathrm{Uniform}(\mathcal{T}), Q_{Z|T}) + \delta)$ for some $\delta > 0$ then Eq. (4) converges to $-\infty$ as $n \to \infty$, which means the eavesdropper Eve has little information on the secret message. This means that if $\ln|\mathcal{L}_n|/n$ converges to $I(\mathrm{Uniform}(\mathcal{T}), Q_{Z|T})$ and the wiretap capacity (1) is achieved with uniform channel input then this construction also achieves the wiretap capacity.

Drawbacks in the proposed construction is the random selection of channel encoders. This requires that almost all pairs of encoder and decoder have to provide low decoding error probability, which is not verified with most of channel codes. Moreover, in some case, for example the channel encoder using the Trellis shaper [8], it is difficult to prepare a family of encoders that satisfies the requirement. Thus, in the next section, we show a deterministic construction of a wiretap code from a given channel code.

IV. Deterministic construction of a wiretap code

In this section, we assume that the index set $\mathcal{G}_n$ has only one element, and we are given a pair of an encoder $\mu_{\mathrm{Alice},n}$ a decoder $\mu_{\mathrm{Bob},n}$. We also assume that the given family $\mathcal{F}_n$ of hash functions satisfies the condition that for all $f \in \mathcal{F}_n$ and $m \in \mathcal{M}_n$ we have $|f^{-1}(m)| = |\mathcal{L}_n|/|\mathcal{M}_n|$ in order to apply Theorem 7 in Sec. V. This assumption on $\mathcal{F}_n$ is satisfied, for example when $\mathcal{M}_n = \mathbf{F}_q^k$ and $\mathcal{L}_n = \mathbf{F}_q^n$, using the set of all the surjective linear maps from $\mathcal{L}_n$ to $\mathcal{M}_n$. Moreover, the linear mappings defined by the concatenation of the identity matrix and the Toeplitz matrix considered in [12, Appendix] also satisfy the assumption and is more efficiently implemented in practice.

The construction of the wiretap code is the same as the previous section except that there is no random selection of encoders. The construction in this section can achieve the wiretap capacity (1) if the distribution P_T on $\mathcal{T}$ realizing (1) also maximizes the mutual information $I(P_T, Q_{Z|T})$ to the eavesdropper. In order to evaluate the average of the mutual information, we develop a new privacy amplification theorem (Theorem 7) based on Gallager function by modifying [11, Lemma 2] in the next section. Applying this result, one can show that

$$I(M_n; Z_n|F_n) \leq \frac{|\mathcal{M}|^s \exp(\phi(s, Q^n_{Z|T}, P_{T_n}))}{|\mathcal{L}|^s s},$$

[1] The concavity is proved under that assumption that $\mathcal{Z}$ is finite. However, if the conditional probability $Q_{Z|X}$ is Gaussian, the concavity proof needs no change except notational ones.

for $0 \le s \le 1/2$, where

$$\begin{aligned}&\phi(s, Q^n_{Z|T}, P_{T_n})\\ = \;& \ln \int_{\mathcal{Z}^n} \left(\sum_{t \in \mathcal{T}^n} P_{T_n}(t) (Q^n_{Z|T}(z|t))^{1/(1-s)} \right)^{1-s} dz.\end{aligned}$$

If $\mathcal{Z}$ is finite, the integration should be replaced by summation and $Q_{Z|T}$ should be interpreted as the conditional probability.

Again, for a given channel encoder $\mu_{\mathrm{Alice},n}$, it is also practically impossible to compute $\phi(s, Q^n_{Z|T}, P_{T_n})$. We shall show that a method to upper bound it. We have

$$\exp(\phi(s, Q^n_{Z|T}, P_{T_n})) \le \max_{P_n} \exp(\phi(s, Q^n_{Z|T}, P_n)),$$

where P_n is a probability distribution on $\mathcal{T}_n$. Observe that ϕ is essentially same as the function E_0 in [1], [9]. Thus if $P_{1,s}$ maximizes $\exp(\phi(s, Q_{Z|T}, P_{1,s}))$, then its n-fold i.i.d. extension $P^n_{1,s}$ also maximizes $\max_{P_n} \exp(\phi(s, Q^n_{Z|T}, P_n))$ [1], and we have

$$I(M_n; Z_n|F_n) \le \frac{|\mathcal{M}|^s \exp(n\phi(s, Q_{Z|T}, P_{1,s}))}{|\mathcal{L}|^s s}. \tag{5}$$

Observe that for fixed s and $Q_{Z|T}$, $\exp(\phi(s, Q_{Z|T}, P_{1,s}))$ is a concave function on a convex set and $P_{1,s}$ can easily be computed [4]. Observe also that for fixed $Q_{Z|T}$, the function $\max_{P_{1,s}}$[RHS of Eq. (5)] is a convex function of s, thus $\min_s \max_{P_{1,s}}$[RHS of Eq. (5)] can also be easily computed by the bisection method [4, Algorithm 4.1].

The logarithm of the right hand side is

$$s\left(\ln |\mathcal{M}_n| - \ln |\mathcal{L}_n| + \frac{n\phi(s, Q_{Z|T}, P_{1,s})}{s} \right) - \ln s.$$

Since ϕ is essentially E_0 in [9], $\lim_{s\to 0} \phi(s, Q_{Z|T}, P)/s = I(P, Q_{Z|T})$, where P is a distribution on $\mathcal{T}$. Let $P_{\max}$ be a distribution on $\mathcal{T}$ maximizing $I(P, Q_{Z|T})$. Therefore, by the almost same argument as Section II, if $\ln |\mathcal{M}_n| < \ln |\mathcal{L}_n| - n(I(P_{\max}, Q_{Z|T}) + \delta)$ for all n, then $I(M_n; Z_n|F_n)$ goes to zero as $n \to \infty$. If $P_{\max}$ also maximizes the wiretap capacity (1) and the given channel code achieves the information rate $I(P_{\max}, Q_{Y|T})$ then the construction in this section achieves the wiretap capacity.

V. New privacy amplification theorem in terms of the Gallager function

We shall show the following new privacy amplification theorem that is indispensable with the deterministic construction of wiretap codes in Sec. IV.

Theorem 7: Assume that the given family of two-universal hash function F from $\mathcal{L}$ to $\mathcal{M}$ satisfies that

$$|F^{-1}(m)| = \frac{|\mathcal{L}|}{|\mathcal{M}|}, \quad \forall m,$$

a fixed conditional probability $Q_{Z|L}$ is given, and the random variable L obeys the uniform distribution on $\mathcal{L}$. Then,

$$I(F(L); Z|F) = \mathrm{E}_F I(F(L); Z) \le \frac{|\mathcal{M}|^s \exp(\bar{\phi}(s, Q_{Z|L}))}{|\mathcal{L}|^s s}, \tag{6}$$

for $0 \le s \le 1/2$, where E_F expresses the expectation concerning the random variable F,

$$\bar{\phi}(s, Q_{Z|L}) = \ln \int_{\mathcal{Z}} \Big(\mathrm{E}_L (Q_{Z|L}(z|L))^{1/(1-s)} \Big)^{1-s} dz$$

and dz is an arbitrary measure.

Proof. Observe first that the joint probability $P_{FL} = P_F \times P_L$ and the conditional probability $Q_{Z|L}$ uniquely determines $Q_{Z|F(L)}$. We can check that the function $s \mapsto \bar{\phi}(s, Q^n_{Z|F(L)})$ satisfies the following properties:

$$\begin{aligned}&\bar{\phi}(0, Q_{Z|F(L)}) = 0, \quad \frac{d^2 \bar{\phi}(s, Q_{Z|F(L)})}{ds^2} \ge 0\\ &\frac{d\bar{\phi}(s, Q_{Z|F(L)})}{ds}\Big|_{s=0} = I(F(L); Z).\end{aligned}$$

Hence, its convexity guarantees the inequality $s\mathrm{E}_F I(F(L); Z) \le \mathrm{E}_F \bar{\phi}(s, Q_{Z|F(L)})$, which implies the inequality

$$\mathrm{E}_F I(F(L); Z) \le \mathrm{E}_F \frac{\bar{\phi}(s, Q_{Z|F(L)})}{s} \tag{7}$$

for $0 < s \le \frac{1}{2}$. In the following, we denote the uniform distriburtion on $\mathcal{L}$ by P_L

Let $1 + u = \frac{1}{1-s}$, then $1 \ge u > 0$ and $s = \frac{u}{1+u}$. Since $x \mapsto x^u$ is concave,

$$\begin{aligned}&\mathrm{E}_F \Big[\sum_{\ell' : F(\ell') = F(\ell), \ell' \ne \ell} Q_{Z|L}(z|\ell') \Big]^u\\ \le& \Big[\mathrm{E}_F \sum_{\ell' : F(\ell') = F(\ell), \ell' \ne \ell} Q_{Z|L}(z|\ell') \Big]^u\\ \le& \Big[\sum_{\ell' : \ell' \ne \ell} \frac{1}{|\mathcal{M}|} Q_{Z|L}(z|\ell') \Big]^u \le \Big[\frac{|\mathcal{L}|}{|\mathcal{M}|} Q_Z(z) \Big]^u = (\frac{|\mathcal{L}|}{|\mathcal{M}|})^u Q_Z(z)^u.\end{aligned} \tag{8}$$

Using (8) and the relation $(x + y)^u \le x^u + y^u$ for two positive real numbers x, y, we obtain

$$e^{\mathrm{E}_F \bar{\phi}(s, Q_{Z|F(L)})} \le \mathrm{E}_F e^{\bar{\phi}(s, Q_{Z|F(L)})} \tag{9}$$

$$\begin{aligned}=&\mathrm{E}_F \int_{\mathcal{Z}} \Big(\sum_{m \in \mathcal{M}} \frac{1}{|\mathcal{M}|} Q_{Z|F(L)}(z|m)^{1+u} \Big)^{\frac{1}{1+u}} dz\\ \le& \int_{\mathcal{Z}} \Big(\mathrm{E}_F \sum_{m \in \mathcal{M}} \frac{1}{|\mathcal{M}|} Q_{Z|F(L)}(z|m)^{1+u} \Big)^{\frac{1}{1+u}} dz \qquad (10)\\ =& \int_{\mathcal{Z}} \Big(\mathrm{E}_F \sum_{m \in \mathcal{M}} \frac{1}{|\mathcal{M}|} Q_{Z|F(L)}(z|m) Q_{Z|F(L)}(z|m)^u \Big)^{\frac{1}{1+u}} dz\\ =& \int_{\mathcal{Z}} \Big(\mathrm{E}_F \sum_{m \in \mathcal{M}} \frac{1}{|\mathcal{M}|} \Big[\sum_{\ell \in \mathcal{L} : F(\ell) = m} \frac{|\mathcal{M}|}{|\mathcal{L}|} Q_{Z|L}(z|\ell) \Big]\\ & \qquad \Big[\sum_{\ell \in \mathcal{L} : F(\ell) = m} \frac{|\mathcal{M}|}{|\mathcal{L}|} Q_{Z|L}(z|\ell) \Big]^u \Big)^{\frac{1}{1+u}} dz\\ =& \int_{\mathcal{Z}} \Big(\mathrm{E}_F \sum_{\ell \in \mathcal{L}} \frac{1}{|\mathcal{L}|} Q_{Z|L}(z|\ell) (\frac{|\mathcal{M}|}{|\mathcal{L}|})^u \Big[Q_{Z|L}(z|\ell)\\ & \qquad + \sum_{\ell' \in \mathcal{L} : F(\ell') = F(\ell), \ell' \ne \ell} Q_{Z|L}(z|\ell') \Big]^u \Big)^{\frac{1}{1+u}} dz\end{aligned}$$

$$\leq \int_{\mathcal{Z}} \Big(\mathrm{E}_F \sum_{\ell \in \mathcal{L}} \frac{1}{|\mathcal{L}|} Q_{Z|L}(z|\ell) (\frac{|\mathcal{M}|}{|\mathcal{L}|})^u \Big[Q_{Z|L}(z|\ell)^u + \big(\sum_{\ell' \in \mathcal{L}: F(\ell')=F(\ell), \ell' \neq \ell} Q_{Z|L}(z|\ell') \big)^u \Big] \Big)^{\frac{1}{1+u}} dz \tag{11}$$

$$= \int_{\mathcal{Z}} \Big((\frac{|\mathcal{M}|}{|\mathcal{L}|})^u \sum_{\ell \in \mathcal{L}} \frac{1}{|\mathcal{L}|} Q_{Z|L}(z|\ell)^{1+u} + \big(\frac{|\mathcal{M}|}{|\mathcal{L}|}\big)^u \times \sum_{\ell \in \mathcal{L}} \frac{1}{|\mathcal{L}|} Q_{Z|L}(z|\ell) \mathrm{E}_F \big(\sum_{\ell \neq \ell' \in F^{-1}(\ell)} Q_{Z|L}(z|\ell') \big)^u \Big)^{\frac{1}{1+u}} dz$$

$$\leq \int_{\mathcal{Z}} \Big((\frac{|\mathcal{M}|}{|\mathcal{L}|})^u \mathrm{E}_L Q_{Z|L}(z|L)^{1+u} + (\frac{|\mathcal{M}|}{|\mathcal{L}|})^u Q_Z(z) \big(\frac{|\mathcal{L}|}{|\mathcal{M}|}\big)^u Q_Z(z)^u \Big)^{\frac{1}{1+u}} dz \tag{12}$$

$$= \int_{\mathcal{Z}} \Big((\frac{|\mathcal{M}|}{|\mathcal{L}|})^u \mathrm{E}_L Q_{Z|L}(z|L)^{1+u} + Q_Z(z)^{1+u} \Big)^{\frac{1}{1+u}} dz$$

$$\leq \int_{\mathcal{Z}} \Big((\frac{|\mathcal{M}|}{|\mathcal{L}|})^u \mathrm{E}_L Q_{Z|L}(z|L)^{1+u} \Big)^{\frac{1}{1+u}} + (Q_Z(z)^{1+u})^{\frac{1}{1+u}} dz \tag{13}$$

$$= \int_{\mathcal{Z}} (\frac{|\mathcal{M}|}{|\mathcal{L}|})^{\frac{u}{1+u}} \Big(\mathrm{E}_L Q_{Z|L}(z|L)^{1+u} \Big)^{\frac{1}{1+u}} + Q_Z(z) dz$$

$$= 1 + (\frac{|\mathcal{M}|}{|\mathcal{L}|})^{\frac{u}{1+u}} \int_{\mathcal{Z}} \Big(\mathrm{E}_L Q_{Z|L}(z|L)^{1+u} \Big)^{\frac{1}{1+u}} dz$$

$$= 1 + (\frac{|\mathcal{M}|}{|\mathcal{L}|})^s e^{\bar{\phi}(s, Q^n_{Z|L})},$$

where the inequalities can be shown in the following way. Ineq. (12) follows from (8). Ineq. (11) and (13) follow from inequality $(x+y)^u \leq x^u + y^u$ for $0 \leq u \leq 1$ and $x, y \geq 0$. Ineq. (10) follows from the concavity of $x \mapsto x^u$ for $0 \leq u \leq 1$. Ineq. (9) follows from the convexity of $x \mapsto e^x$. Since the above inequality implies

$$\mathrm{E}_F \bar{\phi}(s, Q_{Z|F(L)}) \leq \ln[1 + (\frac{|\mathcal{M}|}{|\mathcal{L}|})^s e^{\bar{\phi}(s, Q^n_{Z|L})}] \leq (\frac{|\mathcal{M}|}{|\mathcal{L}|})^s e^{\bar{\phi}(s, Q^n_{Z|L})},$$

using (7) we obtain (6).

VI. Conclusion

In this paper, starting from an arbitrary given channel code, we showed two constructions of wiretap codes. The first one involves the randomized selection of channel encoders. The second one is deterministic. These two construction can achieve the wiretap capacity under different conditions. Our constructions provide the strong security.

Ideally, the addition of hash functions to an arbitrary given channel code should always achieve the wiretap capacity whenever the given channel code achieves the capacity of the composition of the artificially added channel $Q_{X|T}$ plus the physical channel $Q_{Z|X}$. The proposed constructions fall short of this ideal. The improved construction should be explored. The numerical computation of an optimal $Q_{X|T}$ from given $Q_{Y|X}$ and $Q_{Z|X}$ is also an open problem.

Acknowledgment

The second author would like to thank Prof. Yasutada Oohama, Prof. Tomohiko Uyematsu, Dr. Shun Watanabe, and Dr. Kenta Kasai for helpful discussions. This research was partially supported by a Grant-in-Aid for Scientific Research in the Priority Area "Deepening and Expansion of Statistical Mechanical Informatics (DEX-SMI)," No. 18079014 and a MEXT Grant-in-Aid for Young Scientists (A) No. 20686026.

References

[1] S. Arimoto, "On the converse to the coding theorem for discrete memoryless channels," *IEEE Trans. Inform. Theory*, vol. 19, no. 3, pp. 357–359, May 1973.

[2] J. Barros and M. Bloch, "Strong secrecy for wireless channels," in *ICITS 2008*, ser. Lecture Notes in Compute Sciences, R. Safavi-Naini, Ed., vol. 5155. Springer-Verlag, 2008, pp. 40–53.

[3] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, "Generalized privacy amplification," *IEEE Trans. Inform. Theory*, vol. 41, no. 6, pp. 1915–1923, Nov. 1995.

[4] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge University Press, 2004.

[5] J. L. Carter and M. N. Wegman, "Universal classes of hash functions," *J. Comput. System Sci.*, vol. 18, no. 2, pp. 143–154, Apr. 1979.

[6] I. Csiszár, "Almost independence and secrecy capacity," *Problems of Information Transmission*, vol. 32, no. 1, pp. 40–47, 1996.

[7] I. Csiszár and J. Köner, "Broadcast channels with confidential messages," *IEEE Trans. Inform. Theory*, vol. 24, pp. 339–348, 1978.

[8] G. D. Forney, Jr., "Trellis shaping," *IEEE Trans. Inform. Theory*, vol. 38, no. 2, pp. 281–300, Mar. 1992.

[9] R. G. Gallager, *Information Theory and Reliable Communication*. New York: John Wiley & Sons, 1968.

[10] M. Hamada, "Security of quotient codes for classical wiretap channels," in *Proc. SITA2009*, Dec. 2009, pp. 309–314.

[11] M. Hayashi, "General non-asymptotic and asymptotic formulas in channel resolvability and identification capacity and its application to wiretap channel," *IEEE Trans. Inform. Theory*, vol. 52, no. 4, pp. 1562–1575, 2006.

[12] ——, "Exponential evaluations in universal random privacy amplification," 2009, arXiv:0904.0308.

[13] D. Klinc, J. Ha, S. M. McLaughlin, J. Barros, and B.-J. Kwak, "LDPC codes for the Gaussian wiretap channel," in *Proc. ITW*, Oct. 2009, pp. 95–99.

[14] S. K. Leung-Yan-Cheong and M. E. Hellman, "The gaussian wire-tap channel," *IEEE Trans. Inform. Theory*, vol. 24, pp. 451–456, Jul. 1978.

[15] Y. Liang, H. V. Poor, and S. Shamai (Shitz), *Information Theoretic Security*. Hanover, MA, USA: NOW Publishers, 2009.

[16] R. Matsumoto, "Problems in application of ldpc codes to information reconciliation in quantum key distribution protocols," 2009, arXiv:0908.2042.

[17] U. Maurer and S. Wolf, "Information-theoretic key agreement: From weak to strong secrecy for free," in *EUROCRYPTO 2000*, ser. LNCS, B. Preneel, Ed. Springer-Verlag, 2000, vol. 1807, pp. 351–368.

[18] J. Muramatsu and S. Miyake, "Construction of wiretap channel codes by using sparse matrices," in *Proc. ITW*, Oct. 2009, pp. 105–109.

[19] R. Renner, "Security of quantum key distribution," *International Journal on Quantum Information*, vol. 6, no. 1, pp. 1–127, Feb. 2008, (originally published as Ph.D thesis, ETH Zürich, Switzerland, 2005).

[20] A. Thangaraj, S. Dihidar, A. Calderbank, S. McLaughlin, and J.-M. Merolla, "Application of ldpc codes to the wiretap channel," *IEEE Trans. Inform. Theory*, vol. 53, pp. 2933–2945, Aug. 2007.

[21] A. D. Wyner, "The wire-tap channel," *Bell System Tech. J.*, vol. 54, pp. 1355–1387, 1975.